

REMARKS

Claims 1-6, 8-19, 21-30 are pending and remain. Claims 1, 2, 14, 21, and 27-30 have been amended. No new matter has been entered.

Rejections under 35 U.S.C. § 103(a) over Thompson, Lee, and Nelson

5 Claims 1-6, 8, 9, 12-19, 21, 22, and 25-30 stand rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 7,027,872, issued to Thompson, in view of U.S. Patent No. 6,442,432, issued to Lee, and U.S. Patent Application Publication No. 2001/0023360, to Nelson et al. ("Nelson"). Applicant traverses.

 The Examination Guidelines for Determining Obviousness Under 35 U.S.C. 103 in View of the Supreme Court Decision in *KSR International Co. v. Teleflex Inc.*, 72 Fed. Reg. 57,526 (Oct. 10, 2007) ("*KSR* Guidelines"), effective October 10, 2007, control obviousness determinations and provide exemplary rationales, as incorporated in MPEP 2143. Rationale (G), which includes some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to 10 modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention, appears to have been applied. Three factual inquiries must be made. 15

 First, a finding must be made that there was some teaching, suggestion, or motivation, either in the references themselves or in the knowledge generally 20 available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. MPEP 2143(G)(1).

 Thompson discloses a medical data management system for encrypting data, including an implantable medical device, programmer, and clinician computer (Thompson, Col. 4, lines 40-44). A first key is generated for the programmer and a 25 second corresponding key is generated for the clinician computer (Thompson, Col. 11, lines 37-41). Sensitive information is sent from the implantable medical device to the programmer for encryption by the first key (Thompson, Col. 8, lines 37-41; Col. 9, lines 10-12). After encryption, the sensitive information is transmitted to the clinician computer (Thompson, Col. 9, lines 64-66). Once received, the clinician 30 computer decrypts the sensitive information using the second key (Thompson, Col.

10, lines 36-42).

In contrast, Lee teaches a data communications system that provides the exchange of data between distributed clinicians (Lee, Abstract). An interface medical unit collects data from an implantable medical device via radio frequency (Lee, Col. 10, lines 50-57). Once obtained, the interface medical unit further transmits the data to a central computer, remote computer, remote medical devices, and remote data communication devices over a collaborative network (Lee, Col. 10, lines 50-57; Col. 11, lines 25-27). The central computer is connected to a storage device for storing clinician and device contact information, historical patient data, and telecommunication device contact information (Lee, Col. 12, lines 18-25 and lines 55-59). The remote computer interacts with the interface medical unit to display information from the central computer and the medical devices. The remote computer also allows clinicians to communicate with other clinicians (Lee, Col. 13, lines 12-22).

In further contrast, Nelson teaches providing real time communication between an implantable medical device and a remote computing device (Nelson, Abstract). A query for data is sent to the implantable medical device (Nelson, paragraph [0073]). If adequate bandwidth exists for the requested data, an implantable medical device network interface ("IMDNI") collects data from the implantable medical device via a radio frequency connection or a telemetry connection (Nelson, paragraphs [0020], [0038], and [0052]). Otherwise, the data transfer fails to occur (Nelson, paragraph [0073]). After receipt of the data, the IMDNI further transmits the data to a remote interrogator for storage and analysis (Nelson, paragraphs [0042] and [0043]). The data is transmitted through a dedicated line, such as a direct dial-up connection or over an internetwork, such as the Internet (Nelson, paragraph [0043]). If the data is transmitted over the Internet, encryption or tunneling will be provided to ensure confidentiality (*Id.*). Preferably, a single encryption scheme is effected from the implantable medical device, through the IMDNI, to the remote interrogator (Nelson, paragraph [0049]). After receipt of the data, the remote interrogator generates notifications, accompanied by relevant

data from the implantable medical device, which are transmitted to remote data devices, including a computer, cellular telephone, or facsimile (Nelson, paragraph [0057]; FIGURE 3). Again, the data is encrypted prior to transmission to the remote data devices (Nelson, paragraph [0057]).

5 The Thompson-Lee-Nelson combination lacks a motivation to combine.
“The motivation to combine may be implicit and may be found in the knowledge of one of ordinary skill in the art, or, in some cases, from the nature of the problem to be solved.” *Dystar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co.*, 464 F.3d 1356, 1366 (Fed. Cir. 2006). Thompson focuses on providing “the
10 differentiation, segregation, and classification of data at required or needed levels of security” (Thompson, Abstract). More specifically, different levels of encryption are automatically provided based on a type of data received (Thompson, Col. 5, lines 58-67). Thus, Thompson provides a solution for reducing the amount of bandwidth needed to encrypt sensitive data by determining a type of the data and a
15 corresponding encryption level for that type of data (Thompson, Col. 4, lines 49-Col. 5, lines 40). For example, data that is classified as less sensitive may be transmitted in unencrypted form or with minimal encryption (Thompson, Col. 5, lines 64-67). Further, each device in Thompson is equipped with an encryption engine that includes a classifier and segregator to determine the level of encryption
20 needed for each type of data transmitted and to encrypt the data.

In contrast, Lee focuses on providing data between distributed clinicians to enable real time communication. Modifying Lee to include data classification for determining a type of encryption would require each device to include an encryption engine with a classifier, which would hinder distributed clinician communication for
25 those clinicians with devices not having the classifier. Further, modifying Nelson to include select encryption, as taught by Thompson, would require each of the remote devices of Nelson to include a classifier. However, Nelson focuses on and teaches real time communication between an implantable medical device and a computing device, which further communicates with remote devices. Including the teachings
30 of Thompson would prevent communication with devices not having a classifier.

The Thompson, Lee, and Nelson references attempt to solve different problems involving different aspects of transferring data. Thompson is focused on selecting data for encryption, as well as selecting a type of encryption, whereas, Lee and Nelson focus on transferring patient data from an implantable medical device to remote devices in real time. As such, one skilled in the art would not be motivated to combine the references. Accordingly, a teaching, suggestion, or motivation to combine Thompson, Lee, and Nelson has not been shown.

Next, a finding that there was a reasonable expectation of success must be made. MPEP 2143(G)(2). The claims have been read on a combination of Thompson, Lee, and Nelson but how the combination would be reasonably expected to succeed has not been explained. "The mere fact that references can be combined or modified does not render the resultant combination obvious unless the results would have been predictable to one of ordinary skill in the art." MPEP 2143.01(III) (citing *KSR International Co. V. Teleflex Inc.*, USPQ2d 1385, 1396 (2007)).

Further, the Thompson-Lee-Nelson combination fails to teach each and every element of the claims. Independent Claims 1, 14, and 27 have been amended. Claim 1 now recites an external source comprising a key module to securely obtain the crypto key over a secure connection from a secure key repository securely maintaining the crypto key and to encrypt the sensitive information using the crypto key, a long range transmission module to transmit the encrypted sensitive information to the implantable medical device via a long range interface and to store the encrypted sensitive information onto the implantable medical device, and a short range transmission module to further transmit a copy of at least a part of the sensitive information to the implantable medical device via a secure short range interface and to store the copy as unencrypted data onto the implantable medical device. Claim 14 recites encrypting the sensitive information using the crypto key, transmitting the encrypted sensitive information to the implantable medical device via a long range interface, and storing the encrypted sensitive information onto the implantable medical device; and further transmitting a copy of at least a part of the sensitive information to the implantable medical device via a secure short range

interface and storing the copy as unencrypted data onto the implantable medical device. Claim 27 recites means for encrypting the sensitive information using the crypto key, means for transmitting the encrypted sensitive information to the implantable medical device via a long range interface, and means for storing the encrypted sensitive information onto the implantable medical device; and means for further transmitting a copy of at least a part of the sensitive information to the implantable medical device via a secure short range interface and storing the copy as unencrypted data onto the implantable medical device. Support for the claim amendments can be found in the specification on page 11, line 25 to page 12, line 4; page 13, lines 14-27; and page 15, line 17 to page 16, line 8. No new matter has been added.

Similarly, Claims 28-30 have been amended. Claim 28 now recites an implantable medical device comprising a receiver to receive sensitive information via a long range interface and a copy of at least a part of the sensitive information via a short range interface and a memory to store the sensitive information encrypted using a crypto key uniquely associated with an implantable medical device and the copy as unencrypted data. Claim 29 recites receiving sensitive information via a long range interface and a copy of at least a part of the sensitive information via a short range interface and storing the sensitive information encrypted using a crypto key uniquely associated with an implantable medical device and the copy as unencrypted data. Claim 30 recites means for receiving sensitive information via a long range interface and a copy of at least a part of the sensitive information via a short range interface and means for storing the sensitive information encrypted using a crypto key uniquely associated with an implantable medical device and the copy as unencrypted data. Support for the claim amendments can be found in the specification on page 11, line 25 to page 12, line 4; page 13, lines 14-27; and page 15, line 17 to page 16, line 8. No new matter has been added.

The claim amendments should not necessitate a new ground of rejection based on prior art not of record, as each of the limitations in the claim amendments

were already considered and examined in the prior Office action. *See* MPEP 706.07(a) (“A second or any subsequent action on the merits in any application or patent involved in reexamination proceedings should not be made final if it includes a rejection, on prior art not of record, of any claim amended to include limitations
5 which should reasonably have been expected to be claimed” (emphasis added)).

The Thompson-Lee-Nelson combination fails to teach simultaneously storing sensitive data as encrypted data and a copy of the sensitive data as unencrypted data on an implantable medical device. Instead, Lee teaches a communication system including an interface medical device and a central
10 computer, which focuses on obtaining data from the implantable medical device and transmitting the data to a central computer, remote medical devices, or data communication devices via the interface medical device (Lee, Col. 10, lines 52-61). The data, such as patient information and implantable medical device instructions is encrypted prior to transmission to ensure patient confidentiality (Lee, Col. 15, lines
15 9-21). One encryption scheme is used for the transmission of data between multiple devices, including the implantable medical device, the interface medical device, and the central computer (Lee, Col. 16, lines 10-17).

To render the data in a useful form for analysis and review by the patient or a physician, the data must be decrypted upon receipt by one of the multiple devices.
20 *See, e.g.,* Lee, Col. 15, lines 50-55. Otherwise, the patient and physician would be unable to comprehend the encrypted data, which is transformed to an unreadable state, without decryption or obtaining a copy of the encrypted data. However, Lee teaches transmitting only the data, which is collected by the implantable medical device, and not generating a copy of the data for simultaneous storage. Thus, Lee
25 teaches encrypting data for transmission to multiple devices and decrypting the data upon receipt for processing, rather than storing sensitive information as encrypted data onto an implantable medical device and further storing a copy at least a part of the sensitive information as unencrypted data onto the implantable medical device.

Nelson further fails to teach simultaneously storing sensitive information in
30 encrypted form and a copy of the sensitive information in unencrypted form.

Instead, Nelson teaches real-time communication of data collected by an implantable medical device (Nelson, Abstract). Data is queried from the implantable medical device. Prior to sending the data, a determination is made as to whether sufficient bandwidth exists for transmission (Nelson, paragraph [0073]). If so, the data is sent to an IMDNI; otherwise, the data is not transferred (*Id.*). Upon receiving the data, the IMDNI transmits the data to a remote interrogator for further transmission to remote devices, such as a cellular telephone, physician computer, or printer (Nelson, paragraph [0047]). Although Nelson focuses on obtaining data from an implantable medical device, Nelson also teaches transmitting instructions from the remote programmer to the implantable medical device (Nelson, paragraph [0059]). The instructions are stored alone, without further accompaniments, such as a copy of the instructions in unencrypted form. *See, for e.g., Id.* Therefore, Nelson fails to teach simultaneously storing sensitive data in encrypted form and a copy of the sensitive data in unencrypted form on an implantable medical device.

Moreover, even if Lee was interpreted to teach storing patient data as encrypted data on an implantable medical device, and Nelson was interpreted to teach storing patient data unencrypted data on an implantable medical device, as described in the Office Action of January 15, 2008 (Office Action, p. 3, lines 1-7), there is no teaching, suggestion, or motivation, which provides that the encrypted data and the unencrypted data include the same data or that the unencrypted data is a copy of the encrypted data. Rather, the Thompson-Lee-Nelson combination would teach storing patient data as encrypted data and further storing other patient data as unencrypted data on an implantable medical device. Separately or in combination, the Thompson, Lee, and Nelson references fail to teach generating a copy of patient data and then simultaneously storing the patient data as encrypted data and the copy as unencrypted data on an implantable medical device.

The Thompson-Lee-Nelson combination further fails to teach transmitting encrypted sensitive information via a long range interface and a copy of the sensitive information via a short range interface. In contrast, Thompson teaches an information exchange network, through which all data is transmitted between an

implantable medical device, programmer, and clinician computer (Thompson, p. 6, lines 56-64; FIGURE 1). Thus, the data is transmitted using a single communication means. Therefore, Thompson teaches a general communications network for transmitting the data, rather than transmitting encrypted sensitive information via a long range interface and a copy of the sensitive information via a short range interface.

Further, Lee teaches establishing radio frequency telemetry between an implantable medical device and an interface medical unit (Lee, Col. 11, lines 18-24; FIGURE 1). A short range telemetry interface can also be established by positioning the patient in proximity with the interface medical unit (Lee, Col. 16, lines 50-62). The data is transmitted between the interface medical unit and the implantable medical device using the radio frequency telemetry *or* the short range telemetry, rather than transmitting the data through one type of communication link and a copy of the data through a different type of communication link. Thus, Lee fails to teach transmitting, to an implantable medical device, encrypted sensitive information through a long range interface and a copy of the sensitive information through a secure short range interface.

Moreover, Nelson teaches performing an interrogation session with an implantable medical device by positioning a patient in proximity with an IMDNI (Nelson, paragraph [0032]) or via radio frequency telemetry (Nelson, paragraph [0020]). Similar to Lee, Nelson teaches using a single telemetry connection to transmit the data. Thus, the data is either collected by the IMDNI via radio frequency telemetry or via a short range telemetry interface. Therefore, Nelson teaches obtaining data from an implantable medical device via a single communication means, rather than transmitting encrypted sensitive information via a long range interface and a copy of the sensitive data via a short range interface.

Moreover, the Thompson-Nelson-Lee combination fails to teach retrieving encrypted data from the implantable medical device.

Finally, additional findings must be made based on *Graham* factual inquiries, as necessary, in view of the facts of the case under consideration, to

explain a conclusion of obviousness. MPEP 2143(G)(A). No further *Graham* factual findings were made.

“If any of [the three] findings cannot be made, then this rationale cannot be used to support a conclusion that the claim would have been obvious to one of ordinary skill in the art.” MPEP 2143(G). Accordingly, a *prima facie* case of obviousness has not been shown with respect to the independent Claims. Claims 2-6, 8, 9, 12, and 13 are dependent upon Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 15-19, 21, 22, 25, and 26 are dependent upon Claim 14 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Withdrawal of the rejection is respectfully requested.

Rejections under 35 U.S.C. § 103(a) over Thompson, Lee, Nelson, and Eckmiller

Claims 10, 11, 23, and 24 stand rejected under 35 U.S.C. § 103(a) as being obvious over Thompson, Lee, and Nelson as applied to Claims 1 and 14 above, and further in view of U.S. Patent No. 6,493,587, issued to Eckmiller et al. (“Eckmiller”). Applicant traverses.

Eckmiller teaches a neuroimplant protection system for preventing unauthorized access to data in a neuroprosthesis (Eckmiller, Abstract). The neuroprosthesis includes an internal component that is embedded in a patent and an external component located (Eckmiller, Col. 3, lines 40-46). During manufacture, a key is assigned to the external component and a corresponding lock is assigned to the internal component (Eckmiller, Col. 3, lines 54-57). An authorization signal, including frequencies and a temporal sequence is also generated during manufacture and assigned to the key and lock combination (Eckmiller, Col. 3, lines 57-67). Communication commences and data is transferred once the authorization signal is transmitted from the external component and reaches the internal component at prescribed times and values (Eckmiller, Col. 4, lines 26-57 and Col. 7, lines 30-36).

Dependent Claim 10 recites wherein the crypto key is maintained on the implantable medical device and the crypto key is retrieved through short range

telemetry. Similarly, Claim 23 recites maintaining the crypto key on the implantable medical device and retrieving the crypto key through short range telemetry. In contrast, Eckmiller teaches asymmetric data encryption using a public and private key system. Each component in the neuroprosthesis system operates a set of keys, including a private key that is known only by that component and a corresponding public key (Eckmiller, Col. 9, lines 30-34). The corresponding public key is also maintained by the other components in the system. During manufacture, each component is provided with a private key and corresponding public key, as well as with the public keys of the other components (Eckmiller, Col. 9, lines 34-36). Thus, each component is already equipped to decrypt the data received from another component, without having to retrieve a crypto key from that other component. Therefore, Eckmiller teaches maintaining a public key on the receiving component to decrypt data, rather than retrieving a crypto key from an implantable medical device, per Claim 10.

Maintaining a crypto key on an implantable medical device would not be predictable from the teachings of Eckmiller, as each component already has a public key for each device and would not therefore need to request one. Eckmiller, though, is limited to only those devices for whom public keys are known, which becomes a barrier to secure communication, should an unknown device be encountered. For example, a transmitting component uses a transmitting private key and a public key of a receiving component to encrypt data, which is then transferred to the receiving component. The receiving component then decrypts the data using the public key of the transmitting component and a receiving public key (Eckmiller, Col. 9, lines 47-49). If the received data was encrypted with keys other than those provided by the manufacturer, the data cannot be decrypted (Eckmiller, Col. 9, lines 50-53). In contrast, the use of a single key, as in Claims 10 and 23, allows devices without a corresponding private key to decrypt received data, subsequent to authentication. The same key is used to encrypt and decrypt the data (Spec., p. 3, lines 10-12; p. 8, lines 21-29; and p. 10, lines 8-11). Therefore, Eckmiller teaches the use of a private key for encryption and a public key for decryption, rather than using the same key

for encryption and decryption. Thus, Eckmiller teaches away. References should not be combined when one of the references teaches away. MPEP 2145(X)(D)(2).

Eckmiller further teaches automatically replacing the public and private keys at random time intervals. Each component automatically passes the replacement
5 public key, which is based on their private key, to the other components after receipt of the replacement public key (Eckmiller, Col. 9, lines 39-41), rather than providing the public key upon initiation of communication by the other components. Further, the transmission of data in Eckmiller fails to occur through short range telemetry, such as inductive telemetry. Short range telemetry includes placing a wand over the
10 location of an implantable medical device to retrieve a crypto key from the implantable medical device (Spec., p. 13, lines 7-13). The communication remains open and data is exchanged without encryption. The close proximity of the wand and the implantable medical device provide sufficient safeguards for open data exchange, even for sensitive information. Instead, Eckmiller teaches protected data
15 transmission channels and biometric channels to transmit the data (Eckmiller, Col. 4, line 64-Col. 5, line 11).

Accordingly, the Thompson-Lee-Nelson-Eckmiller combination fails to render Claims 10 and 23 obvious. Additionally, Claims 10 and 11 are dependent upon Claim 1 and are patentable for the above-stated reasons, and as further
20 distinguished by the limitations therein. Claims 23 and 24 are dependent upon Claim 14 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Withdrawal of the rejection is requested.

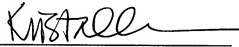
The prior art made of record and not relied upon has been reviewed by the applicant and is considered to be no more pertinent than the prior art references
25 already applied.

Further consideration and examination of the application are respectfully requested. Claims 1-6, 8-19, and 21-30 are believed to be in a condition for allowance. Entry of the foregoing amendments is requested and a Notice of Allowance is earnestly solicited. Please contact the undersigned at (206) 381-3900
30 regarding any questions or concerns associated with the present matter.

Respectfully submitted,

Dated: May 12, 2008

By:



Krista A. Wittman, Esq.
Reg. No. 59,594

Cascadia Intellectual Property
500 Union Street, Suite 1005
Seattle, WA 98101

Telephone: (206) 381-3900
Facsimile: (206) 381-3999

OA Resp 2